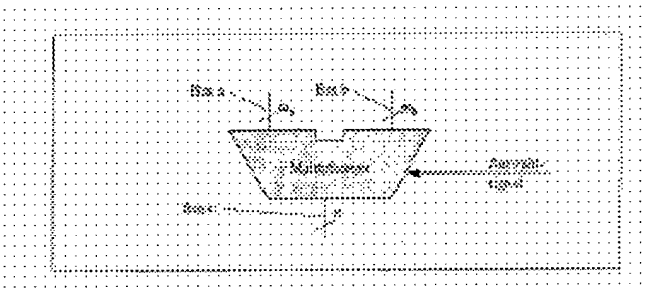
Circuit for digital multiplier assembly for processing binary numbers or Galois Field numbers

Publication number: DE19644688
Publication date: 1998-04-30
Inventor: DRESCHER WOLFRAM DIPL ING (DE); FETTWEIS GERHARD PROF DR ING (DE)
Applicant: UNIV DRESDEN TECH (DE)
Classification:
- international: ***G06F7/52; G06F7/72;*** **G06F7/48; G06F7/60;** (IPC1-7): G06F7/52
- european: G06F7/53; G06F7/72F
Application number: DE19961044688 19961028
Priority number(s): DE19961044688 19961028

Abstract of **DE19644688**

The circuit single logical group is controlled by switch over logic which performs multiplications of binary numbers or of elements of GF(2m). A bus system of the multiplier assembly feeds in two numbers and, for the Galois multiplication, an additional primitive polynomial, and extracts a product. For performing multiplication of two elements of GF(2m), certain transfer lines between the adders/compressors inside the circuit elements for adding the partial products are set to a defined potential. The changeover between the two multipliers is achieved by switching the transfer signal on and off.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 44 688 A 1**

(51) Int. Cl.[6]: G 06 F 7/52

(21) Aktenzeichen: 196 44 688.0
(22) Anmeldetag: 28. 10. 96
(43) Offenlegungstag: 30. 4. 98

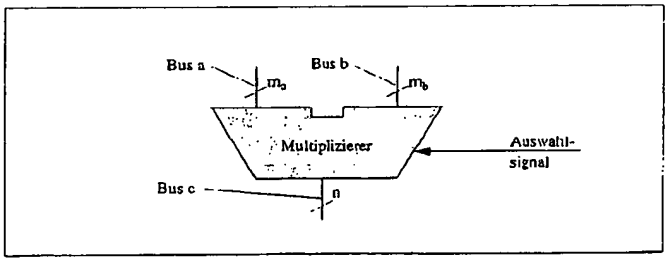
(71) Anmelder:
Technische Universität Dresden, 01069 Dresden, DE

(72) Erfinder:
Drescher, Wolfram, Dipl.-Ing., 01099 Dresden, DE;
Fettweis, Gerhard, Prof. Dr.-Ing., 01324 Dresden, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Schaltungsanordnung einer digitalen Multiplizierer-Baugruppe, zur Verarbeitung von Binärzahlen sowie Elementen aus GF(2≈)

(57) Die Erfindung betrifft eine Schaltungsanordnung einer digitalen Multiplizierer-Baugruppe, zur Verarbeitung von Binärzahlen sowie Elementen aus GF(2^m). Die Schaltungsanordnung ist dadurch gekennzeichnet, daß eine einzige logische Baugruppe auf einem integrierten Schaltkreis, gesteuert durch eine Umschaltlogik, Multiplikationen von Binärzahlen oder von Elementen GF(2^m) ausführt, wobei ein Bussystem der Multiplizierer-Baugruppe zwei Zahlen und für die Galois-Multiplikation zusätzlich ein primitives Polynom zuführt und ein Produkt abführt. Mit der Schaltungsanordnung lassen sich Multiplikationen in den zwei angegebenen Zahlensystemen durchführen, die bestimmte Zellen für beide Multiplikationstypen wiederverwendet. Ein Bussystem zur Verteilung von Daten auf mehrere Multiplizierer-Baugruppen ist somit nicht notwendig.



DE 196 44 688 A 1

Beschreibung

Die Erfindung betrifft eine digitale Schaltungsanordnung zur Multiplikation zweier binär kodierter Zahlen. Dabei ist die Schaltungsanordnung in der Lage, Binärzahlen oder Zahlen aus einem sogenannten Galois-Feld zu verarbeiten. Die Wahl des zu verarbeitenden Zahlenformates erfolgt mittels eines Auswahlsignals. Die Anordnung ist zellular aufgebaut und benutzt größtenteils die selben Zellen zur Berechnung des Produktes beider Zahlenformate.

Multiplizierer, die eines der beiden Zahlenformate verarbeiten können, wurden bereits beschrieben. In B.A. Laws, C.K. Rushforth: A Cellular-Array Multiplier for GF(2^m). IEEE Transactions on Computers, Dezember 1971, S. 1573–1578 wurde ein zellular aufgebauter Multiplizierer für Elemente aus GF(2^m) angegeben. Multiplizierer für Binärzahlen wurden u. a. in K. Hwang: Computer Arithmetic-Principles, Architecture and Design. John Wiley (1979) beschrieben.

Nachteilig bei diesen Anordnungen ist, daß sie nur eines der beiden angegebenen Zahlenformate verarbeiten können. Ist eine Schaltungsanordnung gefordert, die sowohl Elemente aus GF(2^m) als auch Binärzahlen verarbeiten kann, müssen die jeweiligen Schaltungsanordnungen separat aufgebaut werden. Ein entsprechendes Bussystem muß in diesem Fall die Faktoren auf die zwei Multiplizierer-Baugruppen verteilen und das Produkt von einer der Baugruppen abholen. Das erfordert zwei getrennte Multiplizierer und die entsprechenden Busverbindungen.

Aufgabe der Erfindung ist es, eine Schaltungsanordnung gemäß dem Blockschaltbild anzugeben, die größtenteils die selben Zellen auf dem elektronischen Schaltkreis benutzt, um eine multiplikative Verknüpfung von Elementen aus GF(2^m) oder Binärzahlen durchzuführen. Die Busse (Bus a, b, c) zur Bereitstellung der Faktoren und zum Abtransportieren des Produktes können dabei die selben sein.

Die Erfindung beruht auf dem gemeinsamen Ausnutzen der logischen Exklusiv-Oder Funktion (⊗). Diese Funktion wird auf der Bit-Ebene sowohl bei der Multiplikation von Binärzahlen (in Form von Voll- und Halbadder Baugruppen), als auch bei der Multiplikation von Elementen aus GF(2^m)zur Addition von partiellen Produkten bzw. zur Modulo-Reduktion verwendet.

Zwei Binärzahlen a und b der Bit-breite m und n sollen mittels einer Logik-Baugruppe multipliziert werden. Dabei werden zuerst n partielle Produkte gebildet, indem jedes einzelne Bit der Zahl b mit der gesamten Zahl a bitweise multipliziert wird, $b_i \cdot a$ ($0 \le i < n$). Die einzelnen partiellen Produkte besitzen eine Wertigkeit 2^i. Anschließend werden alle n partiellen Produkte unter Berücksichtigung ihrer Wertigkeit zum Endergebnis, dem Produkt, addiert. Das geschieht bitweise unter Verwendung von logischen Volladder- oder Halbadder-Baugruppen. Im Falle es werden mehrere Bits (u. U. auch mit verschiedener Wertigkeit) addiert, werden solche Baugruppen auch als Kompressor bezeichnet.

Zwei Elemente aus GF(2^m) g und h der Bitbreite m können multipliziert werden, indem zuerst jedes einzelne Bit der Zahl h mit der gesamten Zahl g bitweise multipliziert wird, $h_i \cdot g$ ($0 \le i < m$), und die entstandenen partiellen Produkte zu einem Zwischenergebnis der Bitbreite 2m–1 addiert werden. Die Addition von Elementen aus GF(2^m) aus einer Körpererweiterung von GF(2) ist durch bitweise Exklusiv-Oder Verknüpfung definiert. Anschließend wird das Zwischenergebnis schrittweise modulo eines primitiven Polynoms p der Bitbreite m+1 auf das Ergebnis der Bitbreite m substituiert. Dieses Verfahren ist u. a. in P.A. Scott et al.: A Fast VLSI Multiplier for GF(2^m). IEEE Journal on Selected Areas in Communications. Vol. 4 (1986), pp. 62–65 beschrieben.

Ein 3-Bit Volladder mit den logischen Funktionen Summe = A ⊗ B ⊗ C und Übertrag = A ∧ B ∨ (A ∨ B) ∧ C beinhaltet im Summen-Pfad zwei Exklusiv-Oder Baugruppen. Eine oder auch mehrere Exklusiv-Oder Baugruppen werden erfindungsgemäß auch zur Addition von zwei korrespondierenden Bits der Elemente aus GF(2^m) genutzt, die durch die logische Exklusiv-Oder Funktion A ⊗ B definiert ist. Werden Kompressor-Baugruppen höherer Ordnung an Stelle der Adder benutzt, können die darin enthaltenen Exklusiv-Oder Baugruppen wie beschrieben verwendet werden. Da eine Multiplizierer-Baugruppe für Binärzahlen aus einer vielfachen Anordnung von Voll- bzw. Halbaddern besteht, deren Übertragsausgänge jeweils mit dem nächsthöherwertigen Bit korrespondieren und bei einer Galois-Multiplizierer Baugruppe keine Überträge benötigt werden, müssen die Übertrags-Leitungen der für beide Arithmetiken benutzten Adder-Zellen abschaltbar sein, zeigt eine Möglichkeit zur Abschaltung des Übertrags-Pfades des Volladders **12** zum Volladder **21** innerhalb eines Volladder-Feldes.

Der Vorteil der erfindungsgemäßen Schaltungsanordnung besteht darin, daß nur eine Baugruppe aufgebaut werden muß um eine Multiplikation in den zwei angegebenen Zahlensystemen durchzuführen die bestimmte Zellen für beide Multiplikations-Typen wiederverwendet. Weiterhin ist kein Bussystem zur Verteilung von Daten auf mehrere Multiplizierer-Baugruppen notwendig.

Nachfolgend wird die Erfindung anhand von zwei Ausführungsbeispielen beschrieben. In den Zeichnungen zeigen:

Fig. 1 das vorgeschlagene Blockschaltbild des erfindungsgemäßen Multiplizierers,

Fig. 2 den prinzipiellen Aufbau der Abschalteinrichtung für das Übertragssignal innerhalb der Addierer-Baugruppe für die Addition der partiellen Produkte,

Fig. 3 der den Anwendungsbeispielen 1 und 2 zugrunde liegende strukturelle Aufbau des Galois-Multiplizierers bezüglich der Addition der partiellen Produkte und der Substitution mittels des primitiven Polynoms,

Fig. 4 das Blockschaltbild der Anordnung nach Ausführungsbeispiel 1 zur Kombination eines Array-Multiplizierers mit einem Galois-Multiplizierer,

Fig. 5 das logische Schaltbild einer Zelle des Arrays **Fig.** 4,

Fig. 6 die schematische Darstellung der Aufteilung in Unterbaugruppen eines 17×17-bit Multiplizierers mit Wallace-Tree-Addition der partiellen Produkte nach Ausführungsbeispiel 2.

Ausführungsbeispiel 1 bezieht sich auf den Aufbau einer kombinierten Multiplizierer-Baugruppe nach dem Prinzip eines u. a. in N.H.E. Weste, K. Eshraghian: Principles of CMOS VLSI Design. Addison-Wesley Publishing Co., Reading, MA. (1993) S. 547 ff. angegebenen Array-Multiplizierers.

Im Ausführungsbeispiel 2 liegt dem kombinierten Multiplizierer ein Baum-orientierter Multiplizierer, wie u. a. in N.H.E. Weste, K. Eshraghian: Principles of CMOS VLSI Design. Addison-Wesley Publishing Co., Reading, MA. (1993) S. 554 ff. beschrieben, zugrunde. In beiden Ausführungsbeispielen wird von der allgemeinen Architektur des Multiplizierers für Binärzahlen ausgegangen und die Architektur des Galois-Multiplizierers darauf zugeschnitten. Ein wesentlicher Unterschied besteht in der Art, wie die Galois Modulo-Reduktion durchgeführt wird. Im Ausführungsbeispiel 1 wird die Modulo-Reduktion direkt auf ein partielles Produkt angewendet, wogegen im Ausführungsbeispiel 2 die Modulo-Reduktion auf alle addierten partiellen Produkte angewendet wird. **Fig.** 3 verdeutlicht diese zwei Verfahren

schematisch.

In der Darstellung ist das Blockschaltbild einer Anordnung nach Ausführungsbeispiel 1 zu sehen. Die Matrix aus gleichartigen Zellen nach **Fig.** 5 ist dunkel unterlegt. Der linke und obere Rand der Matrix wird mit UND-Gattern aufgefüllt. Die Zu- und Abführung der Datenbusse an die Matrix ist durch beschriftete Rechtecke veranschaulicht. In der Baugruppe "MSB Primitives Polynom" wird die höchste Stelle des primitiven Polynoms entweder automatisch durch eine Logik oder durch setzen des entsprechenden Bits in einem Register festgestellt und der Matrix zugeführt. Die Leitungen der Zelle in **Fig.** 5 haben folgende Bedeutung:

a_1, b_i – Bits der Faktoren a, b,
f_i – korrespondierendes Bit im primitiven Polynom,
pp, msb – höchste Stelledes primitiven Polynoms,
sel – Selektionssignal für Multiplikationsart,
y_{ein} – Signal, daß der Zelle anzeigt, ob höchste Stelle im Primitiven Polynom bereits gefunden wurde,
y_{aus} – Signal, daß der nachfolgenden Zelle anzeigt, daß höchste Stelle im Primitiven Polynom bereits gefunden wurde,
sum_gal – Summensignal bei der Galois-Multiplikation,
sum_int – Summensignal bei der Multiplikation von Binärzahlen,
übg Übertragssignal bei der Multiplikation von Binärzahlen.

In **Fig.** 5 ist die kombinierte Nutzung der Exklusiv-Oder Gatter ersichtlich. Führt das sel-Signal L-Pegel, ist die Zelle auf Galois-Multiplikation geschaltet und der Summen-Pfad geht über sum_gal(ein), Mux1, G1, G2, G8, Mux3 nach sum_gal(aus). Liegt am sel-Signal H-Pegel, ist die Zelle in den Binärzahl-Modus geschaltet und der Summen-Pfad führt durch sum_int(ein), Mux1, G1, G2, Mux3 nach sum_int(aus). Über die Faktor-Leitungen a_i, b_i wird in G3 in beiden Modi ein partielles Produkt auf Bitebene gebildet.

Eine andere Anordnung zum Addieren von partiellen Produkten ist eine von C.S. Wallace: A Suggestion for a Fast Multiplier. IEEE Transactions on Computers, Vol. EC13, pp 14–17 (1964) beschriebene Baum-Struktur von Adder-Baugruppen. Zur Kombination dieses Verfahrens mit einem Galois-Multiplizierer kann die in **Fig.** 3 rechts dargestellte Methode zur Modulo-Reduktion benutzt werden. Neu ist dabei die Aufteilung in 2 getrennte Arrays, deren Zellen wiederum Exklusiv-ODER Gatter enthalten. Durch die Aufteilung des Wallace-Baum-Adders in zwei Teil-Bäume gleicher Größe wird die Breite der zu verarbeitenden Galois-Faktoren auf maximal 1/2 der Breite der Binärzahl-Faktoren begrenzt. Die Aufteilung des gesamten Arrays erfolgt folgendermaßen:

1) Ausgangspunkt stellt das Array zur Addition der partiellen Produkte bei der Binär-Multiplikation dar.
2) Dieses Array wird dermaßen entworfen, daß mindestens zwei identische Teilanordnungen entstehen, die die gleiche Anzahl von partiellen Produkten addieren können. Im Falle einer in **Fig.** 6 dargestellten Fallstudie eines 17×17-bit Binär-Multiplizierers empfiehlt sich beispielsweise eine Aufteilung in zwei je 8 partielle Produkte addierende Teilanordnungen und ein nicht in die Konstruktion mit einbezogenes partielles Produkt. Zur Ausführung der Binär-Multiplikation müssen die drei somit entstandenen Teilergebnisse in einer weiteren Teilanordnung addiert werden.
3) Die zwei identischen Teilanordnungen werden zur Verarbeitung der Galois-Multiplizierer-Funktionen Addition Modulo 2 der partiellen Produkte und Reduktion mittels primitivem Polynom genutzt.

Die Teilanordnung Array 1 führt die bitweise Multiplikation und die Addition der partiellen Produkte durch. Aufgrund einer gleichen algorithmischen Struktur können Galois- sowie Binär-Multiplizierer dieselbe Teilanordnung nutzen, ausgenommen der Übertragspfade. Diese Pfade müssen mit einer geeigneten Anordnung gemäß **Fig.** 2 zur Durchführung der Galois-Multiplikation abgeschaltet werden. Am Ausgang der Teilanordnung Array 1 in **Fig.** 3 rechts liegt im Galois-Modus ein Wert an, der alle Modulo 2 summierten partiellen Produkte repräsentiert. In der Teilanordnung Array 2 in **Fig.** 3 rechts wird die Substitution mittels des primitiven Polynomes p durchgeführt. Dabei muß die zur Ausführung der Galois-Multiplikation notwendige Anordnung an die Anordnung des Binär-Multiplizierers in geeigneter Weise adaptiert werden. Das geschieht für die Galois-Anordnung folgendermaßen:

1) Aufteilung des Adder-Arrays in einen linken und einen Rechten Teilbereich.
2) Im linken Teilbereich wird jede Stelle, die größer als des benutzte Galois Feld ist, festgestellt und anhand korrespondierenden Stelle im primitiven Polynom p ausgewertet.
3) Die generierten Signale werden über Rückführungsleitungen aus dem Array herausgeführt und über die Zeileneingänge Faktor b_{22} dem rechten Teilbereich des Array 2 zugeführt.
4) Im rechten Teilbereich von Array 2 findet eine Modulo 2 Addition mit den im verwendeten Galois-Feld liegendem Teil des von Array 1 gelieferten Zwischenergebnisses statt.

Wie in **Fig.** 6 dargestellt ist das Ergebnis der Galois-Multiplikation auf den niederwertigen Bitleitungen des Binär-Zwischenergebnisses von Array 2 bereits vor dem Gesamt-Addierer-Block sichtbar und wird dort bereits abgegriffen. Die Binärmultiplikation benötigt den Gesamt-Adder, um das Endergebnis im getrennten Übertrag-Summe-Format zu berechnen und den Summe-Übertrag Vektor-Addierer um das binäre Endergebnis zu formen.

Patentansprüche

1. Schaltungsanordnung einer digitale Multiplizierer-Baugruppe, zur Verarbeitung von Binärzahlen sowie Elementen aus $GF(2^m)$; **dadurch gekennzeichnet,** daß eine einzige logische Baugruppe auf einem Integrierten Schaltkreis, gesteuert durch eine Umschaltlogik, Multiplikationen von Binärzahlen oder von Elementen $GF(2^m)$ ausführt, wobei ein Bussystem der Multiplizierer-Baugruppe zwei Zahlen und für die Galois-Multiplikation zusätzlich ein primitives Polynom zuführt und ein Produkt abführt.
2. Die Schaltungsanordnung nach Anspruch 1, dadurch gekennzeichnet, daß zur Durchführung der Multiplikation zweier Elemente aus $GF(2^m)$ bestimmte Übertragsleitungen zwischen den Addern/Kompressoren innerhalb der Schaltungselemente zur Addition der partiellen Produkte auf ein festes Potential gelegt und das Umschalten zwischen den zwei Multiplizierern im Wesentlichen durch An- und Abschalten des Übertragssignales erfolgt.
3. Schaltungsanordnung nach Anspruch 1, dadurch gekennzeichnet, daß eine Anzahl von logischen Exklusiv-Oder Zellen sowohl für die Berechnung eines Produktes aus zwei Binärzahlen, als auch für die Berech-

nung eines Produktes zweier Elemente aus GF(2^m) vorgesehen sind, wobei die Exklusiv-Oder Zellen in den Addern/Kompressoren der Schaltungsanordnung zur Addition der partiellen Produkte enthalten sind.

4. Schaltungsanordnung nach Anspruch 1, dadurch gekennzeichnet, daß die logische Baugruppe der Addition der partiellen Produkte im Binär-Multiplizierer, aufgebaut nach dem bekannten Wallace-Tree Verfahren, in mindestens zwei funktionell gleiche Teil-Bäume aufgeteilt ist, die einerseits die Modulo 2-Addition der partiellen Produkte und andererseits die Substitution mittels primitivem Polynom des Galois-Multiplizierers beinhalten.

Hierzu 5 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 196 44 688 A1
Int. Cl.[6]: G 06 F 7/52
Offenlegungstag: 30. April 1998

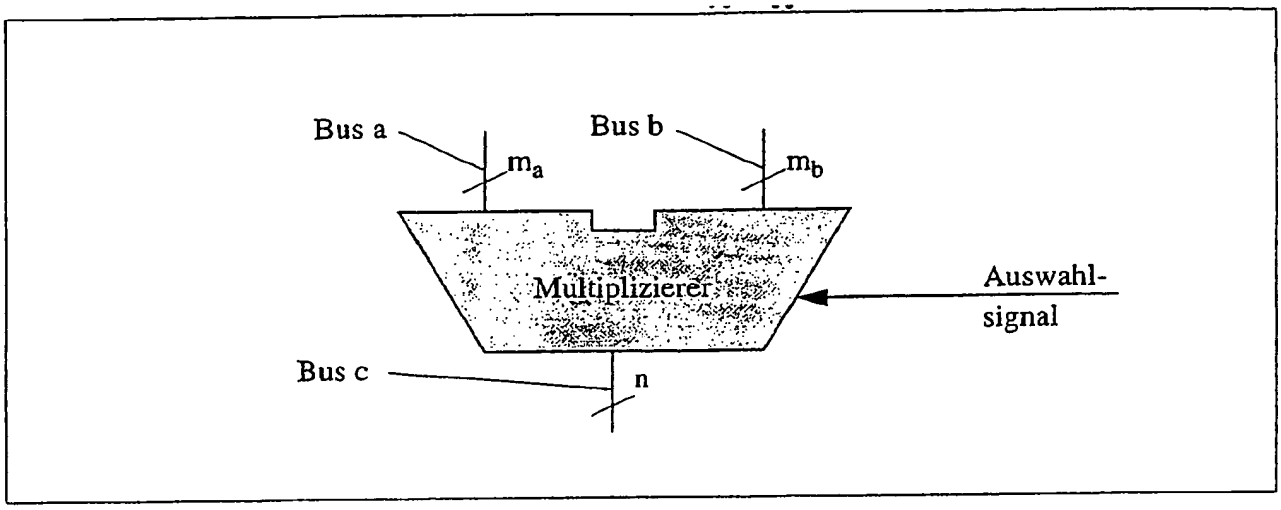


Fig. 1

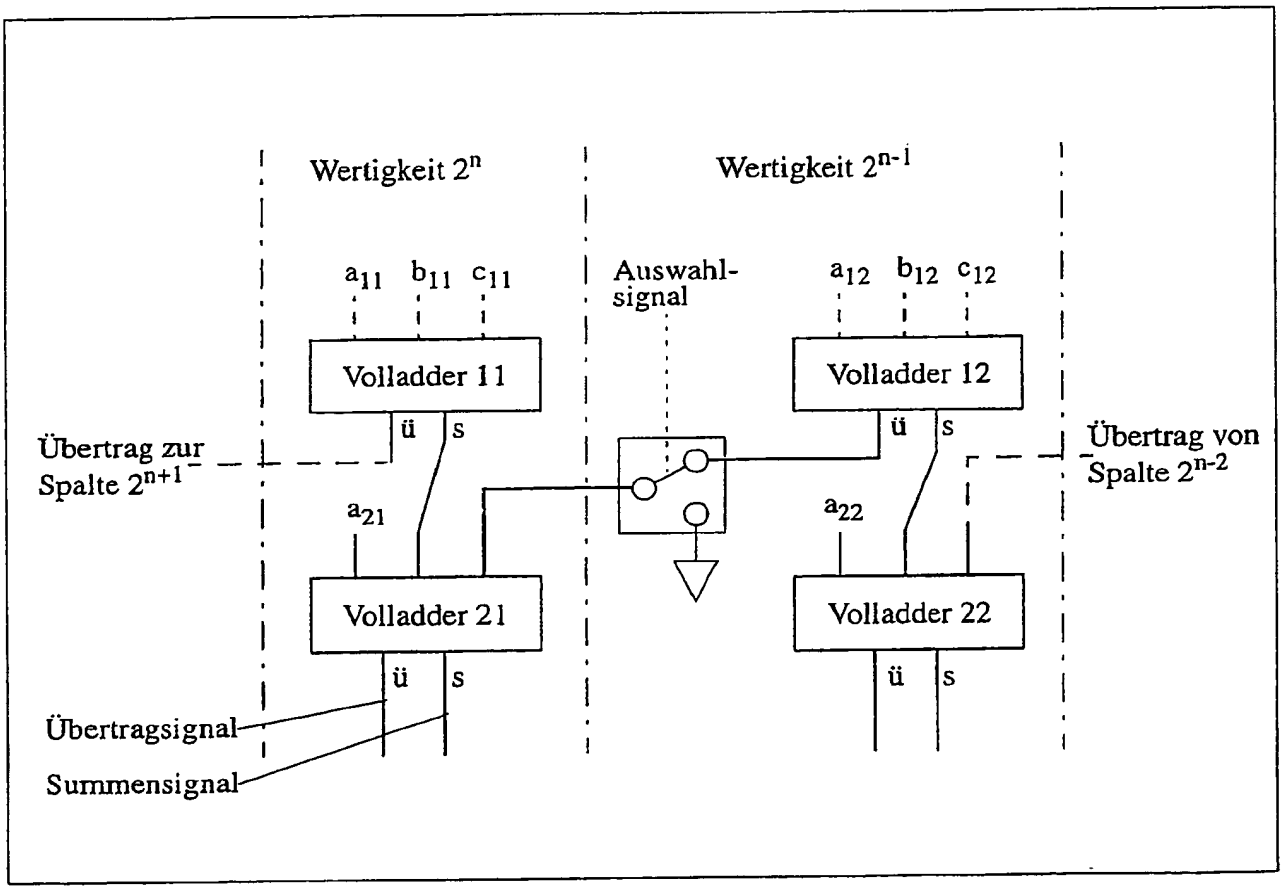


Fig. 2

Nummer: DE 196 44 688 A1
Int. Cl.[6]: G 06 F 7/52
Offenlegungstag: 30. April 1998

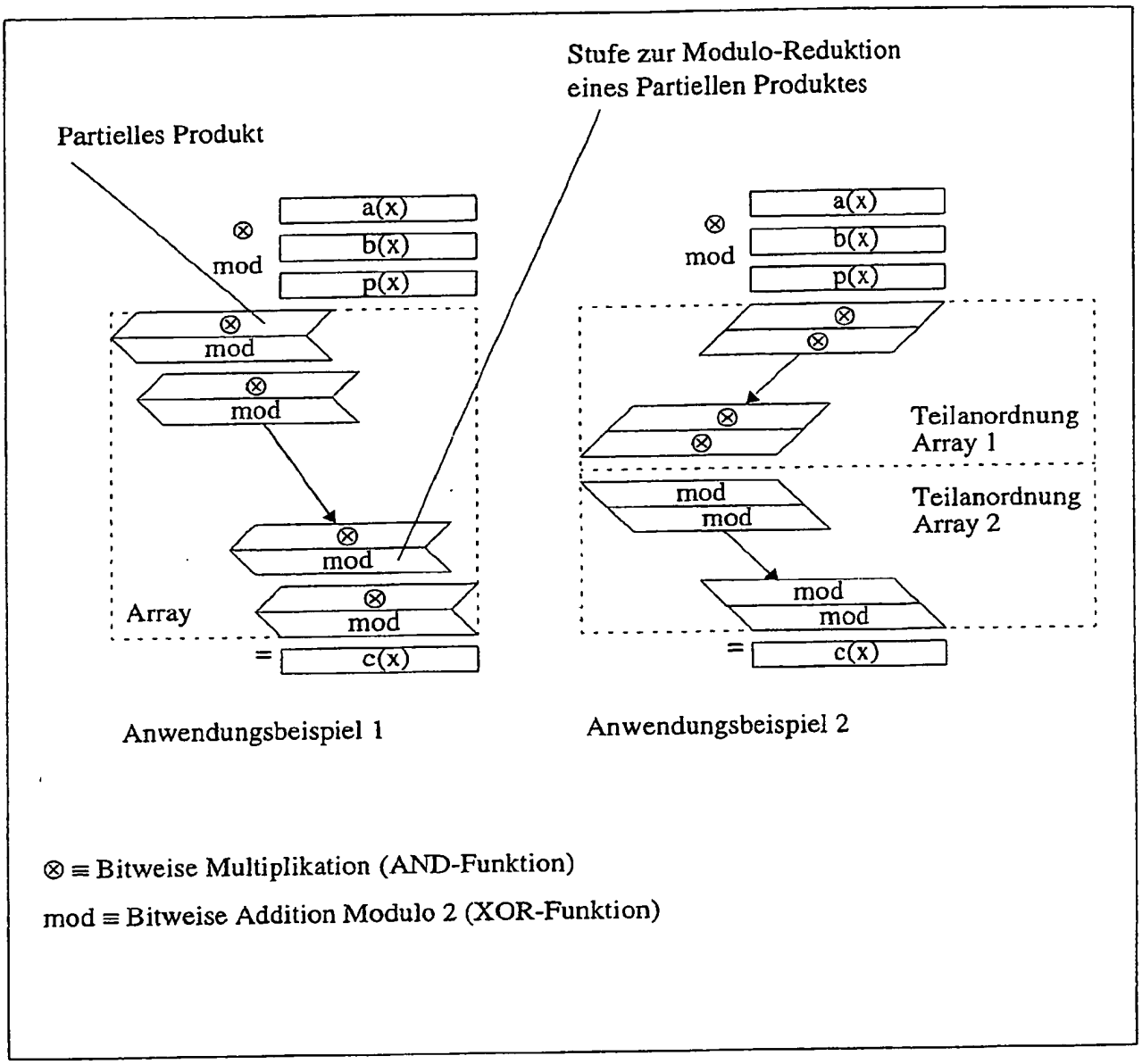


Fig. 3

Nummer: DE 196 44 688 A1
Int. Cl.[6]: G 06 F 7/52
Offenlegungstag: 30. April 1998

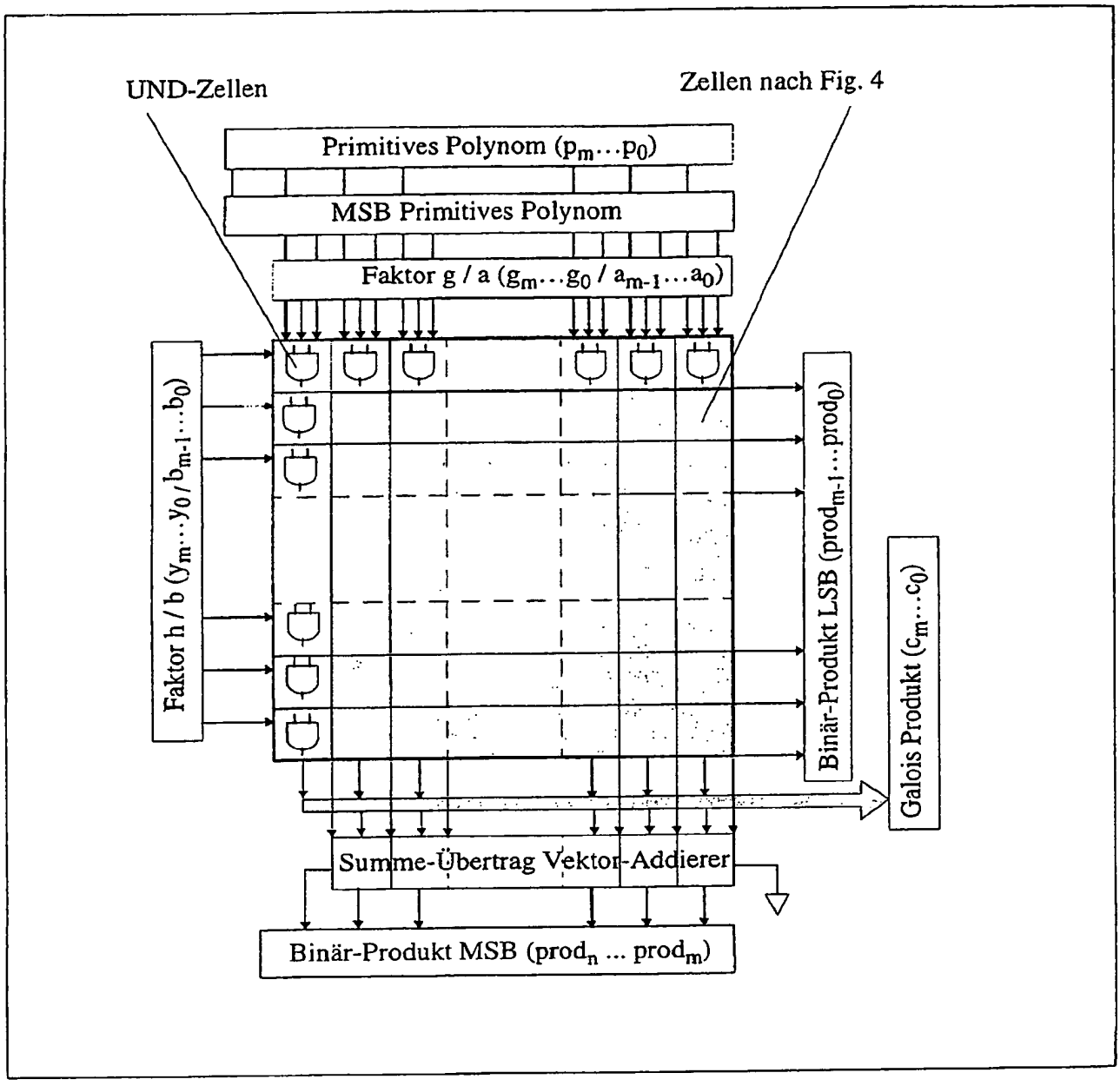


Fig. 4

Nummer: DE 196 44 688 A1
Int. Cl.[6]: G 06 F 7/52
Offenlegungstag: 30. April 1998

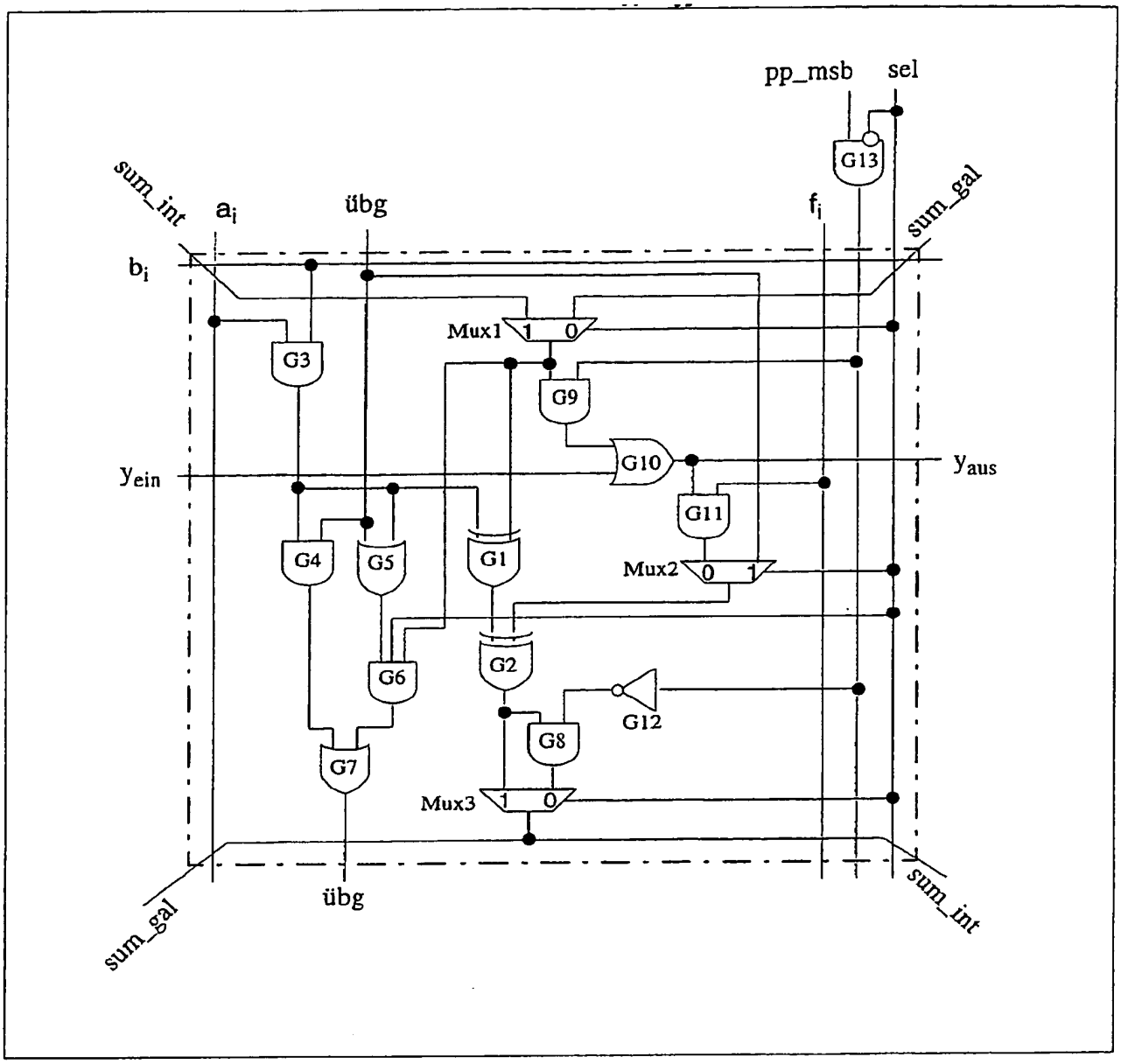


Fig. 5

Nummer: DE 196 44 688 A1
Int. Cl.[6]: G 06 F 7/52
Offenlegungstag: 30. April 1998

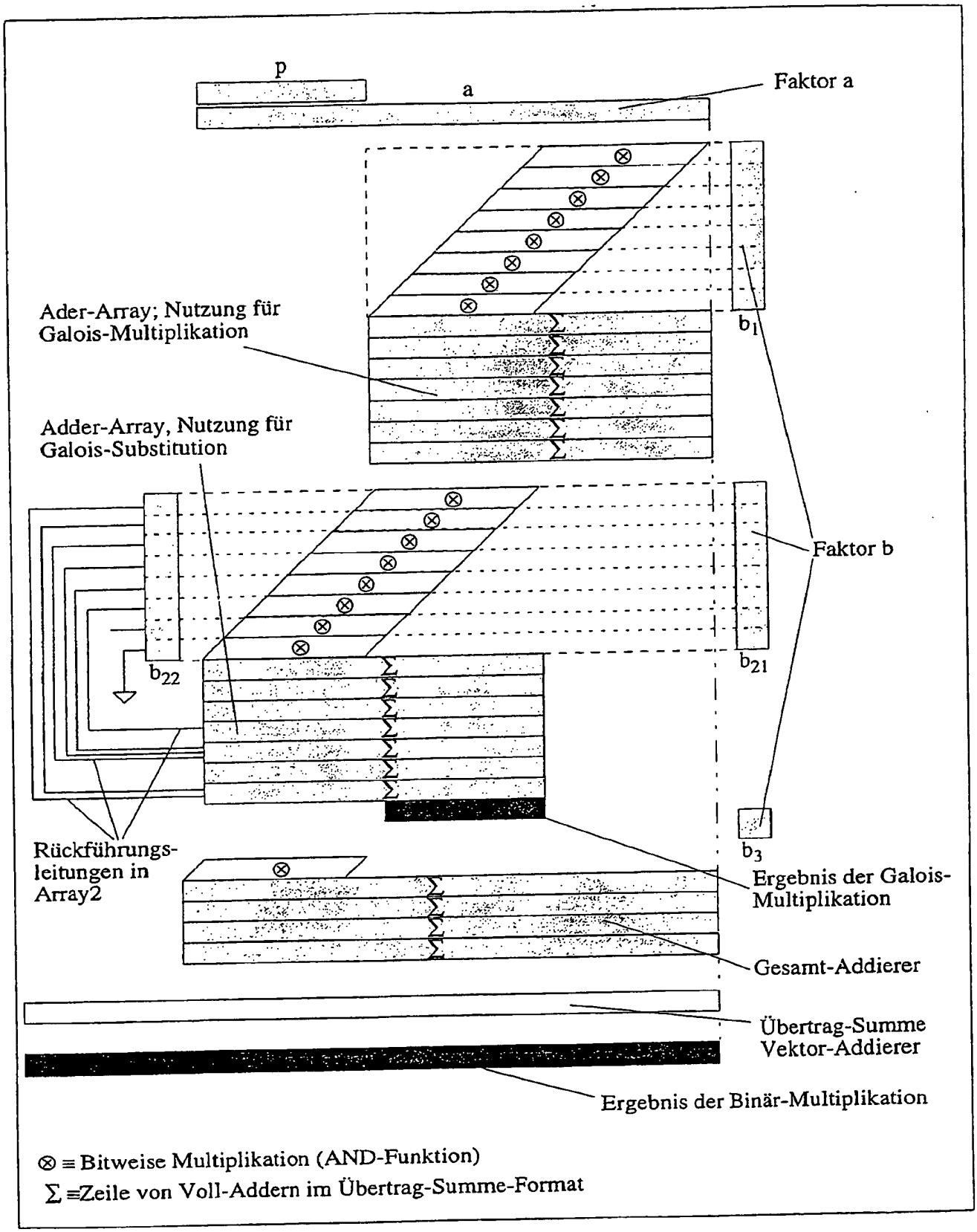


Fig. 6